ALL DIFFERENCE FAMILY STRUCTURES ARISE FROM GROUPS

TIM BOYKETT

Abstract. Difference families are traditionally built using groups as their basis. This paper looks at what sort of generalised difference family constructions could be made, using the standard basis of translation and difference.

The main result is that minimal requirements on the structure force nothing that groups cannot give, at least in the finite case. Thus all difference families arise from groups.

1. Introduction

Difference families are used to construct 2–designs. They are based upon groups, usually additively written. The essential operations are the difference operation and the translation. The differences need to remain invariant under translation.

Quasigroups and loops are generalisations of groups that do not require the operation to be associative. A *quasigroup* is a 2–algebra $(S, +)$ such that for all $a, b \in S$ all equations

$$a + x = b \quad y + a = b$$

have unique solutions for x and y. The Cayley tables of such algebras form Latin squares. There are many special cases of such algebras. In particular a *loop* is a quasigroup with a two–sided identity $e \in S$. A group is an associative loop. See for instance [4].

Quasigroups can be obtained by twisting a group in some way. A simple example is to take an additive group $(G, +)$ and to use the subtraction operation to obtain a quasigroup $(G, -)$ that is not associative. For another example, given a field K, let $k \in K$, $k \neq 0, 1$ be arbitrary but fixed. Define $a * b = ka + (1 - k)b$. Then $(K, *)$ is a quasigroup, in general nonassociative.

There exists a more general form of equivalence between quasigroups, or more general algebras. Two groupoids $(S, +)$ and $(T, *)$ are *isotopic* if there exist bijections $\alpha, \beta, \gamma : S \to T$ such that for all $a, b \in S$ $\alpha(a + b) = \beta(a) * \gamma(b)$. An isomorphism is an isotropism with all bijections identical.

The isotope of a quasigroup is a quasigroup. In particular, many quasigroups are isotopic to groups.

In the following we will first look at difference families and determine what properties are needed to have in order to be useful for such a construction. We demonstrate that such a structure is equivalent to a class of quasigroups. We will then look at this class of algebras and see that they are all simply obtained from groups. The difference family structures come directly from that group. Our main results are Proposition 17 which gives an explicit construction of all such quasigroups and Proposition 18 demonstrating that the difference families are identical.

In general we are only interested in finite structures. However, almost all the results here also apply for infinite structures. We will note the use of finiteness arguments, which are only used in section 3.

2. Difference Families

A *(set) 2–design* is a pair $(V, \mathcal{B})$, where $\mathcal{B}$ is a set of subsets of V all of size k and for all pairs $a, b \in V$, $a \neq b$, $|\{B \in \mathcal{B} : a, b \in B\}| = \lambda$ for some constants k and λ. The number 2 in the name refers to the pairs of elements a, b. There are many variations on this definition, see e.g. [1] for details.

Given a (2)–algebra $(N, +)$ and a set of subsets $\mathcal{B}$ of N, define *development* of $\mathcal{B}$ in N $dev(\mathcal{B})$ to be the collection $\{B + n : B \in \mathcal{B}, n \in N\}$, possibly containing duplicates. The set development is the collection with no duplicates.

Given a group $(N, +)$, not neccesarily abelian, and a set $\mathcal{B} = \{B_i | i = 1, \ldots, s\}$ of subsets of N, called *base blocks*, such that

- all B_i have the same size
- for all $B, C \in \mathcal{B}$, $n \in N$, $B + n = C \Leftrightarrow B = C$ and $n = 0$
- there exists some λ such that for all nonzero $d \in N$, $|\{(B, a, b) | B \in \mathcal{B}, a, b \in B, a - b = d\}| = \lambda$

Then N and B form a *difference family*, (DF).

Theorem 1 (see e.g. [1])**.** *Let $\mathcal{B}$ be a difference family on a group $(N, +)$. Then $dev\mathcal{B}$ is a set 2-design.*

In the proof of this result, we can see that the requirement that $(N, +)$ be a group is too strong. We are only using the translation property and the difference operation. Thus it would seem that this construction can be generalised to be based upon other structures. The following result does this.

Theorem 2. *Let N be a set with binary operation $-$ (difference) and unary operations $t_i \in T$ (translations) and $\mathcal{B}$ a set of subsets of N such that*

- *for all $a, b \in N$ there is a unique t_i such that $t_i a = b$.*
- *for all $a, b \in N$, the equation $a - x = b$ has a unique solution.*
- *$a - b = t_i a - t_i b$ for all $a, b \in N$, for all t_i.*
- *there exists some λ such that for all $d \in N$ such that $d = a - b$ for some $a, b \in N$, $\Delta(d) = \{(B, a, b) | B \in \mathcal{B}, a, b \in B, a \neq b, a - b = d\}$, $|\Delta(d)| = \lambda$*
- *there exists some integer k such that $|t_i B| = k$ for all t_i for all $B \in \mathcal{B}$.*
- *$t_i B = t_j C$ for $B, C \in \mathcal{B}$ implies $i = j$ and $B = C$.*

Then $dev\mathcal{B} = \{t_i B : B \in \mathcal{B}\}$ is a set 2-design.

Proof. All the blocks in $dev\mathcal{B}$ have size k by construction. They are all distinct by the final requirement. We need only show that the number of blocks on a pair of points is constant.

Let $a \neq b \in N$. We show that $|\Delta(a - b)| = |\{t_i B : t_i \in T, B \in \mathcal{B}, a, b, \in t_i B\}|$. There are exactly λ triples (B, α, β) in $\Delta(a - b)$ such that $\alpha, \beta \in B$, $\alpha - \beta = a - b$. For each (B, α, β) in $\Delta(a - b)$ there is a unique t_i such that $t_i \alpha = a$. We know

$$a - b = \alpha - \beta = t_i \alpha - t_i \beta = a - t_i \beta$$

so by the unique solution property of difference, $b = t_i \beta$. Thus $a, b \in t_i B$, so we have a mapping Θ from $\Delta(a - b)$ into $\{t_i B : t_i \in T, B \in \mathcal{B}, a, b, \in t_i B\}$. This map Θ is injective by the final condition.

We now show that Θ is surjective. Let $a, b \in t_i B$. Then there exist some $\alpha, \beta \in B$ such that $a = t_i \alpha$, $b = t_i \beta$,

$$\alpha - \beta = t_i \alpha - t_i \beta = a - b$$

so $(B, \alpha, \beta) \in \Delta(a - b)$, and $t_i B$ is in the image of Θ. Thus Θ is a bijection and we are done. $\square$

We now have a generalised form of difference family. In the next sections we will investigate the algebraic properties underlying this result.

3. Algebraic Properties

Let us investigate the algebraic properties of the results above. For this section, let N, t_i and $-$ be as defined in Theorem 2 above.

Lemma 3. *There exists a unique t_0 that is the identity mapping on N.*

Proof. Fix $a \in N$. By the unique solution property of translations, there is some $t_0 \in T$ such that $t_0 a = a$. Then for all $b \in N$, $a - b = t_0 a - t_0 b = a - t_0 b$, so by the unique solution property of differences, $t_0 b = b$ and t_0 is the identity map on N. □

Theorem 4. *If N is finite then $(N, -)$ is a quasigroup.*

Proof. We know $a - x = b$ has a unique solution. Suppose $x - a = b$ has two solutions, $x_1 \neq x_2$. There is some t_i such that $t_i x_1 = x_2$. Then

$$x_1 - a = t_i x_1 - t_i a = x_2 - t_i a = x_2 - a = b$$

Then $x_2 - x = b$ has solutions a and $t_i a$ for x. Thus $t_i a = a$ so t_i is the identity and $x_1 = x_2$ thus $x - a = b$ has at most one solution. By finiteness, it has exactly one solution, so $(N, -)$ is a quasigroup. □

Definition 5. *Fix $a_0 \in N$. For all $b \in N$, let $t_b \in T$ such that $t_b a_0 = b$. This is unique. Define $x + y := t_y x$.*

Theorem 6. *If N is finite then $(N, +)$ is a quasigroup.*

Proof. By the uniqueness property above, $a + x = b$ has a unique solution. Suppose $x + a = b$ has two solutions x_1, x_2. Then $x_1 - x_2 = (x_1 + a) - (x_2 + a) = b - b$. There is some unique k such that $b + k = x_1$. Then $x_1 - x_2 = b - b = (b + k) - (b + k) = x_1 - x_1$ so $x_1 = x_2$ by quasigroup property of $(N, -)$, so $x + a = b$ has at most one solution. By finteness it has exactly one, and $(N, +)$ is a quasigroup. □

Thus we have shown that the structure used in Theorem 2 can be seen as a set with two operations that form quasigroups. We formalise this, as it is clear that from such a pair of quasigroups, we can form the translations used in Theorem 2.

Definition 7. *A* difference family biquasigroup (DFBQ) $(N, +, -)$ *is a $(2, 2)$–algebra where each operation gives a quasigroup and the equation $a - b = (a + c) - (b + c)$ is satisfied.*

Lemma 8. *A DFBQ has a right additive identity. There is a constant $e \in N$ such that $e = a - a$ for all a.*

Proof. Let $a, \bar{a} \in N$ such that $a + \bar{a} = a$. Then for any b,

$$b - a = (b + \bar{a}) - (a + \bar{a}) = (b + \bar{a}) - a.$$

By the quasigroup property, $b = b + \bar{a}$. This works for all a, b, so $\bar{a}$ is constant, and this constant is a right identity with respect to addition. This identity is unique by the quasigroup property.

Fix some $a \in N$. Define $e := a - a$. For all $b \in N$, there exists some c such that $a + c = b$. Thus $b - b = (a + c) - (a + c) = a - a = e$ and the second statement is proved. □

Note that the first part also follows from Lemma 3 above. We may write a DFBQ as $(N, +, -, o, e)$ where o is a right additive identity and $e = a - a$ for all a.

4. In general

In this section we examine the structure of a general DFBQ. We will use these results in the next section to demonstrate that a general DFBQ is isotopic to a group and that the resulting designs are identical.

Definition 9. *A collection $\mathcal{B}$ and a DFBQ $(N,+,-)$ such that:*

- *there exists an integer k such that $|B|=k$ for all $B\in\mathcal{B}$*
- *there exists some λ such that for all $d\in N$ such that $d=a-b$ for some $a,b\in N$, $\Delta(d)=\{(B,a,b)|B\in\mathcal{B},\, a,b\in B,\, a\neq b,\, a-b=d\}$, $|\Delta(d)|=\lambda$*
- *$B+b=C+c$ for $B,C\in\mathcal{B}$, $b,c\in N$ implies $B=C$ and $b=c$.*

is called a quasigroup difference family (QDF)

It is clear that such a QDF will give a 2-design using the same methods as Theorem 2.

Proposition 10. *Let $(N,+,-,o,e)$ be a DFBQ. Let $\bar{e}$ be such that $e+\bar{e}=o$, then define $\phi : x\mapsto x+\bar{e}$ and $\alpha : x\mapsto x-e$. Define the operations*

$$a\oplus b = \phi^{-1}(\phi a+\phi b) \tag{1}$$
$$a\ominus b = \alpha^{-1}(a-b) \tag{2}$$

Then $(N,\oplus,\ominus,e,e)$ is a DFBQ with $a\ominus e=a$ for all $a\in N$.

Proof. $(N,\oplus)$ and $(N,\ominus)$ are quasigroups by isotopism. Note that $\phi a-\phi b=a-b$ by the DFBQ property, so $\phi^{-1}a-\phi^{-1}b=a-b$. Then

$$\begin{aligned}
(a\oplus c)\ominus(b\oplus c) &= \alpha^{-1}((a\oplus c)-(b\oplus c) && (3)\\
&= \alpha^{-1}((\phi a+\phi c)-(\phi b+\phi c)) && (4)\\
&= \alpha^{-1}(\phi a-\phi b)=\alpha^{-1}(a-b) && (5)\\
&= a\ominus b && (6)
\end{aligned}$$

so we have the DFBQ property. The constants are both e as given by $a\oplus e=\phi^{-1}(\phi a+\phi e)=\phi^{-1}(\phi a+o)=a$ and $a\ominus a=\alpha^{-1}(a-a)=\alpha^{-1}(e)=e$.

The second claim is seen by $\alpha a=a-e$ thus $a\ominus e=\alpha^{-1}(a-e)=a$. □

Note that $a\ominus b=\phi a\ominus\phi b$. This will be important for the next result.

Proposition 11. *Let $(N,\oplus,\ominus,e,e)$ be a DFBQ with $a\ominus e=a$ for all $a\in N$, ϕ a permutation of N such that $a\ominus b=\phi a\ominus\phi b$, α a permutation of N such that $\alpha e=e$. Define*

$$a+b = \phi(\phi^{-1}a\oplus\phi^{-1}b) \tag{7}$$
$$a-b = \alpha(\phi^{-1}a\ominus\phi^{-1}b) \tag{8}$$

Let $o:=\phi e$. Then $(N,+,-,o,e)$ is a DFBQ, $\alpha : a\mapsto a-e$, $\phi : a\mapsto a+\bar{e}$ where $e+\bar{e}=o$.

Proof. $(N,+)$ and $(N,-)$ are quasigroups by isotopism. The DFBQ property is seen by

$$\begin{aligned}
(a+c)-(b+c) &= \alpha(\phi^{-1}\phi(\phi^{-1}a\oplus\phi^{-1}c)\ominus\phi^{-1}\phi(\phi^{-1}b\oplus\phi^{-1}c)) && (9)\\
&= \alpha((\phi^{-1}a\oplus\phi^{-1}c)\ominus(\phi^{-1}b\oplus\phi^{-1}c)) && (10)\\
&= \alpha(\phi^{-1}a\ominus\phi^{-1}b) && (11)\\
&= a-b && (12)
\end{aligned}$$

The constants are given by $a+o=\phi(\phi^{-1}a\oplus\phi^{-1}o)=\phi(\phi^{-1}a\oplus e)=a$ and $a-a=\alpha(a\ominus a)=\alpha e=e$.

Then $\alpha(a) = \alpha(a \ominus e) = \alpha(\phi^{-1}a \ominus \phi^{-1}e) = a - e$. Let $\bar{e}$ be such that $e + \bar{e} = o$. Then $e + \bar{e} = \phi(\phi^{-1}e \oplus \phi^{-1}\bar{e}) = o = \phi e$ so $\phi^{-1}e \oplus \phi^{-1}\bar{e} = e$. Then

$$\begin{aligned}
a = a \ominus e &= \phi^{-1}a \ominus \phi^{-1}e && (13)\\
&= (\phi^{-1}a \oplus \phi^{-1}\bar{e}) \ominus (\phi^{-1}e \oplus \phi^{-1}\bar{e}) && (14)\\
&= (\phi^{-1}a \oplus \phi^{-1}\bar{e}) \ominus e && (15)\\
&= \phi^{-1}a \oplus \phi^{-1}\bar{e} && (16)\\
&= \phi^{-1}(a + \bar{e}) && (17)
\end{aligned}$$

Thus $\phi a = a + \bar{e}$ and we are done. □

We will need the following for the final results.

Definition 12. *A quasigroup* $(Q, \circ)$ *is a* Ward quasigroup *if* $(a \circ c) \circ (b \circ c) = a \circ b$ *for all* $a, b, c \in Q$.

Theorem 13 ([6])**.** *Let* $(Q, \circ)$ *be a Ward quasigroup. Then there exists a unique element* $e \in Q$ *such that for all* $x \in Q$, $x \circ x = e$. *Define* $\bar{x} = e \circ x$ *and* $x * y = x \circ \bar{y}$ *for all* $x, y \in Q$. *Then* $(Q, *, \bar{\ })$ *is a group, and* $x \circ y = x * \bar{y}$.

Proposition 14. *Let* $(N, +, -, e, e)$ *be a DF biquasigroup with* $a - e = a$ *for all* a. *Then it is isotopic to a DF group.*

Proof. Let I be the permutation of N such that $a + Ia = e$. Then

$$a - b = (a + Ib) - (b + Ib) = (a + Ib) - e = a + Ib. \tag{18}$$

Thus $(a - b) - (c - b) = (a + Ib) - (c + Ib) = a - c$ so $(N, -)$ is a Ward quasigroup. Thus there is a group $(N, *, \cdot^{-1})$ with $a - b = a * b^{-1}$ and $a + b = a * (I^{-1}b)^{-1}$ by equation (18). □

The converse of this result holds too. The proof is simple calculation.

Lemma 15. *Let* $(N, *, 1)$ *be a group,* I *a permutation of* N *fixing* 1. *Define*

$$\begin{aligned}
a + b &= a * (Ib)^{-1} && (19)\\
a - b &= a * b^{-1} && (20)
\end{aligned}$$

Then $(N, +, -, 1, 1)$ *is a DF biquasigroup with* $a - 1 = a$ *for all* a.

Thus we obtain information on the form of the map ϕ in Proposition 11. We know the form of the operations from Prop 14 so we can make some explicit statements about the structure.

Corollary 16. *Let* $(N, \oplus, \ominus, e, e)$ *and* ϕ *be as for Proposition 11. Let the operation* $*$ *be as from Prop 14. Then there exists some* $k \in N$ *such that the map* ϕ *is of the form* $\phi(a) = a * k$.

Conversely, given $(N, \oplus, \ominus, e, e)$ *as in Prop 11 and a group operation* $*$, *select any element* $k \in N$. *Then* $\phi(a) := a * k$ *satisfies the requirements of Prop 11.*

Proof. By Prop 14 we know that $a \ominus b = a * b^{-1}$. Since $\phi a \ominus \phi b = a \ominus b$ we have $\phi a * (\phi b)^{-1} = a * b^{-1}$. Let $b = 1$ and we obtain $\phi a * (\phi 1)^{-1} = a$ so $\phi a = a * \phi 1$. Letting $k := \phi 1$ we are done.

The converse is seen by taking any element $k \in N$. Define $\phi a := a * k$. Then $\phi a \ominus \phi b = (a * k) * (b * k)^{-1} = a * b^{-1} = a \ominus b$ so we are done. □

5. General Explicit Descriptions

In this section, we will look at explicit descriptions of DFBQs and QDFs. Using the results above, we know the structure of all DFBQs.

Proposition 17. *Let $(N, *, 1)$ be a group. Let α, β be permutations of N, $\alpha 1 = 1$. Define*

$$a + b = a * \beta b \tag{21}$$

$$o = \beta^{-1}(1) \tag{22}$$

$$a - b = \alpha(a * b^{-1}) \tag{23}$$

Then $(N, +, -, o, 1)$ is a DFBQ and all DFBQs are of this form.

Proof. The forward direction is a calculation and is clear. Let $(N, +, -, o, e)$ be a DFBQ. We demonstrate that there exists a group structure $(N, *, ^{-1}, 1)$ and permutations α, β of N as above.

By Proposition 10 there exist ϕ and α such that defining

$$a \oplus b := \phi^{-1}(\phi a + \phi b) \tag{24}$$

$$a \ominus b := \alpha^{-1}(a - b) \tag{25}$$

we obtain $(N, \oplus, \ominus, e, e)$ is a DFBQ with $a \ominus e = e$. By Proposition 14 there exists some group $(N, *, ^{-1}, 1)$ such that $e = 1$, $a \ominus b = a * b^{-1}$ and $a \oplus b = a * (I^{-1}(b))^{-1}$. Thus

$$a + b = \phi(\phi^{-1} a * (I^{-1}(\phi^{-1} b))^{-1}) \tag{26}$$

$$a - b = \alpha(a * b^{-1}) \tag{27}$$

By Corollary 16 we know that $\phi x = x * k$, $\phi^{-1} x = x * k^{-1}$. Thus

$$a + b = ((a * k^{-1}) * (I^{-1}(b * k^{-1}))^{-1}) * k \tag{28}$$

$$= a * k^{-1} * (I^{-1}(b * k^{-1}))^{-1} * k \tag{29}$$

$$= a * \beta(b) \tag{30}$$

where $\beta(x) = k^{-1} * (I^{-1}(x * k^{-1}))^{-1} * k$ is a permutation of N. Since $a + \beta^{-1}(1) = a * \beta(\beta^{-1}(1)) = a * 1 = a$ we know $\beta^{-1}(1)$ is the unique right identity, so $o = \beta^{-1}(1)$. The permutation α fixes e which is seen to be 1 and we are done. □

This final result shows that all difference family structures are in fact group structures.

Proposition 18. *The quasigroup development and the group development of a difference family are identical.*

Proof. Suppose we have a QDF $\mathcal{B}$ on a DFBQ $(N, +, -, o, e)$. By Prop 17 above, we know that there is a group operation $*$ and some permutation of N such that $a + b = a * \beta(b)$. Thus if B is a subset of N,

$$dev_+ B = \{B + n : n \in N\} = \{B * \beta(n) : n \in N\} = \{B * n : n \in N\} = dev_* B$$

so we obtain exactly the same set of sets. Thus $dev_+ \mathcal{B} = dev_* \mathcal{B}$ and we are done. □

6. Conclusion

It would be desirable to generalise the definition of a difference family so as to use more general structures to derive designs using this formalism. With simple and reasonable requirements for our difference family structures, we have shown that we obtain a biquasigroup algebra and that such algebraic structures must be isotopic to groups. It is also seen that the resulting designs are identical.

Questions remain open as to whether the requirements that we posit are all necessary. It may be reasonable to use a simpler structure for the difference operation, but I cannot see how.

Applications remain open here. For instance, planar nearrings have been shown to possess a difference family structure. Questions about nonassociative planar nearrings have been raised, and it might be appropriate to use these results to deduce structure about the nearrings that could be so defined. It also remains open as to the properties of infinite generalised difference families, where the translations and difference operation do not form a proper quasigroup. The investigation of neardomains and K–loops [3] suggests that there are some strange and interesting properties when we drop the finiteness restriction. In particular there may be connections between the generalisation of nearfields to neardomains and the generalisation to planar nearrings and Ferrero pairs [2, 5], which may be connected to the construction of nonassociative difference families.

7. Acknowledgements

This work has been supported by grant P15691 of the Austrian National Science Foundation (Fonds zur Förderung der wissenschaftlichen Forschung). I would also like to thank Petr Vojtechovsky for many ideas and support with loops and quasigroup theory.

References

[1] Thomas Beth, Dieter Jungnickel, and Hanfried Lenz. *Design theory. Vol. I.* Cambridge University Press, Cambridge, second edition, 1999.
[2] James R. Clay. *Nearrings: Geneses and applications*. Oxford University Press, 1992.
[3] Hubert Kiechle. *Theory of K-loops*. Number 1778 in Lecture Notes in Mathematics. Springer Verlag, 2002.
[4] Hala O. Pflugfelder. *Quasigroups and Loops: Introduction*. Number 7 in Sigma Series in Pure Mathematics. Heldermann, 1990.
[5] Günter Pilz. *Near–rings*. Number 23 in Mathematics Studies. North–Holland, 1983.
[6] Petr Vojtechovsky. Ward quasigroups. Unpublished manuscript, 2003.